Abstract

An object of the present invention is to provide a smart card and a settlement terminal by which when common-key cryptography is used for value transfer between smart cards, the security of the whole system can be improved by enabling easy update of a cryptographic key used for the value transfer.

A smart card transmits/receives value data to/from another smart card. The smart card includes information accumulating means for accumulating the value data, a transfer key used to update the value data, and an update key used to update the transfer key; communication means for receiving a transfer key encrypted by use of the update key, the transfer key being transmitted from another smart card; and arithmetic processing means for decrypting the encrypted transfer key by use of the update key to update the transfer key accumulated in the information accumulating means by use of the decrypted transfer key.